ABSTRACT:

A variant on the 'One Time Pad' cipher is used to provide an encrypted link between two or more stations. The main feature of this variant is the use of a unique and easily created Pseudo-Random Number Sequence segment not having any internal repeats. At one station, a mixing function is used to combine a locally created stream of truly random bytes with a portion of this unique PRNS segment, yielding a fresh stream of truly random data. This freshly created stream of truly random data is operated on in such a way as to create a new and unique PRNS element set which is used to control the functioning of a PRNS generator. The PRNS generator is used to create a new and unique PRNS segment which has a repeat period much longer than the length of the PRNS element set used to create it. It is then useful to treat the PRNS element set as a message and transfer it across the encrypted link to other stations. In this fashion, this OTP cipher variant can be re-keyed and used for as long as there is a continuing source of truly random data available at one of the stations on the network. This technique of using unique and freshly created PRNS segments rather than the classic One Time Pad allows encrypted networks to function independently of any central key distribution regimens or Public Key Infrastructures, making such an encrypted network proof against security breaches perpetrated upon, or key escrow schemes propagated through, such external key distribution infrastructures. This technique also provides certain securities against willful betrayals by tempted users or coerced revelations by users under duress.